**REMARKS:**

Claims 1-13 are in the case and presented for consideration.

Claims 1-2, and 6-7, 9, 11-13 are currently amended

Title:

The Applicants have amended the title in response to the Examiner's objection under MPEP 606.01 at page 2 of the Office Action. The title is now believed to be clearly indicative of the invention to which the claims are directed. Withdrawal of the objection to the title is, therefore, respectfully requested.

Drawings:

The Applicants have provided a replacement sheet 2 with labels indicating the steps of the method disclosed in this application. Support for the changes to replacement sheet 2 may be found on page 5 of the Specification, lines 27-34 and page 6 of the Specification, lines 1-3. No new matter is added.

Claims:

The claims have been amended to recite "users" in the place of "sources" so as to further clarify the scope of the relevant claims. Some language has been modified to place the claims in proper grammatical form in light of the above stated substitution. Claim 13 has been amended to recite patentable subject matter and clarify which statutory class of

invention it belongs to. No new matter has been added.

**Claim Rejection Under 35 U.S.C. § 112, Second Paragraph**

The Examiner has rejected Claim 2 under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner specifically alleges that it is not clear how the "encrypted inner product" as recited in claim 2 is calculated. The Applicants respectfully traverse the rejection for the reasons that follow.

The preferred method of calculating the encrypted inner product is disclosed on page 13, second paragraph of the Specification which describes the protocol for computing similarities on encrypted data. The example assumes that the user-based measure of similarity is the modified form of the Pearson correlation coefficient (Eq. 1) substituting the expression:

$$q_{ut} = \begin{cases} r_{ui} - \overline{r}_u & \text{if } b_{ui} = 1, \text{ i.e., user } u \text{ rated item } i \\ 0 & \text{otherwise,} \end{cases}$$

to eliminate the need for the iterator t of Eq. 1 which is an unknown quantity in the cryptosystem. This results, as the Applicants have stated on page 13 of the Specification, in a rewriting of the Pearson correlation coefficient (Eq. 1) into "a form consisting of **three inner products**, each between a vector of u and one of v."

According to the disclosure, the protocol consists of the first user *u* calculating the vectors of encrypted entries for all permutations of $q_{ut}$ for all $t \in I$ using Eq. 10 (of the Paillier system) and sends these vectors to the server, which forwards the vectors unto the other users. Each recipient user, in turn, will calculate the three inner products necessary to compute the similarity values shown on page 13 of the Specification using a homomorphic encryption scheme such as Eq. 11 (of the Paillier system). These inner products between the vectors of first user *u* and each additional user $v_j$, $j = 1,...,m-1$ are disclosed on page 13 of the Specification as follows:

$$\varepsilon\left(\sum_{t\in I} q_{ut} q_{v_j t}\right), \varepsilon\left(\sum_{t\in I} q_{ut}^2 b_{v_j t}\right), \varepsilon\left(\sum_{t\in I} q_{v_j t}^2 b_{ut}\right)$$

The three equations above are in the form of the dot product of two vectors and the dot product is the standard inner product of the Euclidean space (see http://en.wikipedia.org/wiki/Dot_product (accessed February 8, 2008)).

These three inner products are then sent back to the first user *u* who can decrypt the results as shown on page 10 of the Specification using the preferred Paillier cryptosystem. The decrypted inner products may then be used to calculate the similarity as determined by the modified Pearson correlation coefficient equation describe above and on page 13 of the Specification.

It must be mentioned that the specification discloses a preferred embodiment of the this protocol, but makes clear that alternate methods of determining similarity are equally applicable such as the mean-square which will require the calculation of four inner products (specification page 13). An exact number of inner products, therefore, is not recited in claim 2. Further, though the preferred embodiment assumes the use of the Paillier cryptosystem, it is clear to one skilled in the art that any homomorphic encryption scheme may be used to equal effect.

In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent. See, e.g., Solomon v. Kimberly-Clark Corp., 216 F.3d 1372, 1379, 55 USPQ2d 1279, 1283 (Fed. Cir. 2000). See also Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings, 370 F.3d 1354, 1366, 71 USPQ2d 1081, 1089 (Fed. Cir. 2004) ("The requirement to 'distinctly' claim means that the claim must have a meaning discernible to one of ordinary skill in the art when construed according to correct principles...Only when a claim remains insolubly ambiguous without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite.").

Definiteness of claim language must be analyzed, not in a vacuum, but in light of:

(A) The content of the particular application disclosure;

(B) The teachings of the prior art; and

(C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made. (MPEP 2173.02)

One ordinarily skilled in the art would be able to discern how to calculate the "encrypted inner product" recited in claim 2 after a reasonable attempt of constructing this language in light of the content of the particular application's disclosure and the teachings of the prior art. Therefore, for the above stated reasons, the Applicant respectfully request that the Examiner withdraw his rejection of claim 2 under 35 U.S.C. § 112, second paragraph.

**Claim Rejection Under 35 U.S.C. § 101**

The Examiner has rejected Claim 13 under 35 U.S.C. § 101 for lack of utility and for covering two statutory classes of invention. The reasons for the Examiner's rejection are found on pages 2-3 of the Office Action. The Applicants have amended the language to address the basis for these rejections and believe the claim to be in allowable form. As such, the Applicants respectfully request that the Examiner withdraw his rejection of claim 13 under 35 U.S.C. § 101.

**Claim Rejection Under 35 U.S.C. § 102(b)**

The Examiner has rejected claims 1, 3-4 and 6-13 under 35 U.S.C. § 102(b) as being anticipated by "Collaberative Filtering with Privacy", a paper by John Carry in the

Proceedings of the 2002 IEEE Symposium on Security and Privacy (Carry). The reasons for the Examiner's rejection are found on pages 3-10 of the Office Action. While not expressly stating that claim 5 was rejected under §102(b), the Examiner did provide argument for rejecting claim 5 as being anticipated by Carry (page 5 of the Office Action), and the Applicants will assume that claim 5 is also being rejected under §102(b) for the reasons stated.

**Claim 3**

The Examiner provided no reason for his rejection of claim 3 under 35 U.S.C. § 102(b). A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The Office action should clearly communicate the findings, conclusions and reasons which support them (MPEP 2106). The Examiner has not met his *prima facie* burden of showing that every limitation recited in claim 3 is found in the Carry reference nor has he clearly communicated his findings and conclusions on point. Therefore, the Applicants respectfully request that the Examiner withdraw his rejection of Claim 3 under 35 U.S.C. § 102(b).

**Claim 1**

The Carry reference does not anticipate claim 1, as currently amended, since Carry

does not teach the limitation "computation means (110, 150,190, 191,199) for performing a computation on the encrypted first and second data to obtain a similarity value between the first and second data" where the encrypted first and second data are from a first and second **user** respectively. Rather, Carry teaches an algorithm whereby a community of users can compute a **public aggregate** of their data that does not expose individual users' data (cf. Abstract; Office Action, page 4). Unlike the recited limitation which requires a computing a similarity value between the data of two **users** the Carry protocol requires computing a similarity value between a user's data and a public aggregate matrix consisting of fully decrypted coefficients of the gradient of the matrix. These decrypted coefficients are calculated as a series of vector additions of user data. One user's data is never sent in encrypted form to any other user in the Carry system, rather all data is first optimized and then added to the collective matrix upon which the similarity computation is made for making a prediction for a particular user.

Carry teaches a local, optimized pre-constructed public matrix *A*, an updating algorithm for updating to a centralized location or "blackboard", a user ratings vector determined using the singular value decomposition of P, and an estimate of the user's preference based on a maximum likelihood formulation (Carry, page 4).

This protocol requires that each user first construct an optimized matrix *A* using a conjugate gradient scheme which reduces the calculation to a series of vector additions of user data (Carry, page 4, 3rd paragraph). The users also compute their contribution to the gradient vector and send them to the blackboard in decrypted form. As detailed on page 7

of Carry, talliers collect the partial decryptions from the clients and combine them to produce decrypted totals which are written to the blackboard as fully decrypted coefficients of the gradient of *A*. Talliers update the estimate of *A* using the decrypted line coefficients and conjugate gradient function. They also compute the partial SVD matrices *D* and *V* required for generating recommendations. As such, Carry necessarily computes a similarity value between a user's data and a public "aggregate" matrix **NOT** between two user's as recited in claim 1. At no time is encrypted data from one user sent to another user through the server and therefore, similarity cannot be calculated as a between two users as recited in claim 1 of the present application. The similarity computation is completely centralized in Carry (user-to-public) and distributed (user-to-user) as claimed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The Examiner has not met his *prima facie* burden of showing that every limitation recited in claim 3 is found in the Carry reference. Therefore, the Applicants respectfully request that the Examiner withdraw his rejection of Claim 1 under 35 U.S.C. § 102(b).

**Claims 4 and 5**

The Carry reference does not anticipate claim 4, since Carry does not teach the limitation "and the server is coupled to a public-key decryption server for decrypting the encrypted inner product in the sums of shares and obtaining the similarity value." The Examiner sites to section 3.2 which advocates the El-Gamal public-key cryptosystem. However, the reference does not state that the server calculating the similarity value between first and second data is to be coupled to a separate public-key decryption server. There are many techniques in practice by which authentic public keys can be distributed, including exchanging keys over a trusted channel, using a trusted public file, using an on-line trusted server, and using an off-line server and certificates (see Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. www.cacr.math.uwaterloo.ca/hac). The Examiner alleges that the Carry reference discloses the "gist" of the encryption scheme as recited in claim 4 and described in the specification. Distilling an invention down to the "gist" or "thrust" of an invention disregards the requirement of analyzing the subject matter "as a whole." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Claim 4 of the present application recites more than a generalized public-key cryptosystem, rather, it claims with specificity the structure and elements of that system and how they are integrated, not only with respect to implementing encryption, but also with respect to implementing collaborative filtering. This specific scheme is not found

in the Carry reference, nor is it implied or inherit therein. As such, the Applicant's respectfully request that the Examiner withdraw his rejection of claim 4 under §102(b). Claims 4 and 5 are dependent from claim 1 and are therefore, also allowable for at least the same reasons.

**Claim 6**

The Carry reference does not anticipate claim 6, as currently amended, since Carry does not teach the limitation of "performaing a computation on the encrypted first and second data to obtain a similarity value between the first and second data so that the first and second data is anonymous to the second and first **users** respectively, the similarity value providing an indication of a similarity between the first and second data" where the data come from a first and second **user** respectively. Rather, Carry teaches an algorithm whereby a community of users can compute a **public aggregate** of their data that does not expose individual users' data (cf. Abstract; Office Action, page 4). Unlike the recited limitation, which requires a computing a similarity value between the data of two users, the Carry protocol requires computing a similarity value between a user's data and a public aggregate matrix consisting of fully decrypted coefficients of the gradient of the matrix. One user's data is never sent in encrypted form to any other user in the Carry system, rather all data is first optimized and then added to the collective matrix upon which the similarity computation is made for making a prediction for a particular user.

Further, the similarity value being used to provide an indication of similarity between the first and second data of Carry, necessarily requires a centralized reference matrix for it calculation and would not function without it. The similarity value obtained in Carry is maximum likelihood formulation that minimizes the expression:

$$|x_i|^2/(2\sigma_x^2)+|n_i|^2/2\sigma_n^2$$

where $n_i = P_i - c_1\left(x_i^T\left(DV^T\right)\right)$, the quadratic minimization of each user's rating vector over $x_i$ (Carry, page 4, 4th paragraph). D and V of the this expression are the matrices derived from the SVD of P as described in Appendix I of Carry (Carry, page 4, 4th paragraph). These D and V values are calculated by the talliers as part of a centralized service for producing predictions for the user's (Carry, Section 4). The user's of Carry's system, therefore, must send their individual encrypted user rating vector for item *i* and allow the centralized server to make a similarity computation against the **aggregate matrix**. At no time are similarity values being determined via exchanging information between users as is recited in claim 6. The similarity computation is completely centralized in Carry and distributed in the present application. This is a important difference between the reference and the present Application.

The Examiner alleges that the Carry reference discloses the "gist" of the similarity computation scheme as recited in claim 6 and described in the specification. Distilling an invention down to the "gist" or "thrust" of an invention disregards the requirement of analyzing the subject matter "as a whole." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). "The

identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The Carry reference does not disclose the specific method of comparing encrypted data from a first and second **user** and deriving a similarity value therefrom. As such, the Applicants respectfully request that the Examiner withdraw his rejection of claim 6 under § 102(b).

Claims 7-10 depend from claim 6 and are, therefore, allowable for at least the same reasons. Withdrawal of the rejection of claims 7-10 under §102(b) is, therefore, respectfully requested.

Claims 11-13

Claims 11-13, as currently amended, have language that parallels that of claims 1 and 6 and are, therefore, allowable for at least the same reasons. The Applicants, therefore, respectfully request that the Examiner withdraw his rejection of claims 11-13 under §102(b).

**Claim Rejection Under 35 U.S.C. § 103(a)**

The Examiner has rejected claims 2 and 3 under 35 U.S.C. § 103(a) as being unpatentable over Carry, in view of the Paillier cryptosystem. In his § 103(a) rejection, the Examiner also implicitly combined the reference of "Application of Dimensionality

Reduction in Recommender System – A Case Study" by Sudrul M. Sarwar et. al. in ACM WebKDD 2000 Web Mining for E-Commerce Workship, 2000 (Sarwar)(Office Action at page 5). The reasons for the Examiner's rejection are found on pages 10-12 of the Office Action. The Applicant respectfully traverse the rejection for the reasons given below.

**Claims 2 and 3**

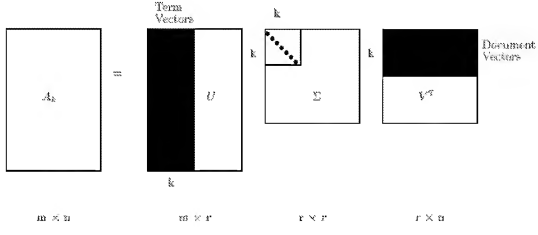
Neither Carry, Sarwar nor the Paillier cryptosystem disclose a the system described in claim 1 wherein the second user calculates, through computational means, an encrypted inner product between the first data and the second data, and provides the encrypted inner product to the first user via the server, the first user decrypting the encrypted inner product for obtaining the similarity value through computational means.

Carry, as discussed, uses the SVD form of the user's rating vector and the aggregate matrix to calculate similarity using maximum likelihood formula never comparing one user's data to another directly. The Sarwar reference relies on a customer-product ratings matrix normalized with naïve non-personalized recommendations (Sarwar, section 3.1.1). The inner product reference by the Examiner is not used to calculate similarity, but rather to compute the recommendation score for any customer *c* and product *p* (Sarwar, section 3.1.1.). The inner product of Sarwar is calculated between the three vectors that are factorized from the *R* matrix using the SVD technique.

The singular value decomposition (SDV) is commonly used in the solution of unconstrained linear least squares problems. Given an $m \times n$ matrix $A$, where without loss of generality $m \geq n$ and rank($A$) = $r$, the SDV of $A$ is defined as:

$A = U\Sigma V^T$,where $U^T U = V^T V = I_n$ and $\Sigma = diag(\sigma_1, \cdots, \sigma_n), \sigma_i > 0$ for $j \geq r+1$.

The first $r$ columns of the orthogonal matrices $U$ and $V$ define the orthonormal eigenvectors associated with the $r$ nonzero eigenvalues of $AA^T$ and $A^T A$, respectively. The columns of $U$ and $V$ are referred to as the left and right singular vectors, respectively, and the singular values of $A$ are defined as the diagonal elements of $\Sigma$ which are the nonnegative square roots of the $n$ eigenvalues of $AA^T$ (see figure below – Berry, M. et al., "Using Linear Algebra for Intelligent Information Retreival". SIAM Review, 74(4), pp. 573-595).




As is clear from the above, the calculation of the inner product is between vectors factorized from the aggregate matrix and not between user data vectors being compared

vis-à-vis each user as disclosed in the present application. Therefore, neither Carry or Sawar teach the limitation of "wherein the **second user** calculates, through computational means, an encrypted inner product between the first data and the second data, and provides the encrypted inner product to the **first user** via the server, the first user decrypting the encrypted inner product for obtaining the similarity value through computational means " recited in Claim 2 of the present application.

In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); Schenck v. Nortron Corp., 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983). Distilling an invention down to the "gist" or "thrust" of an invention disregards the requirement of analyzing the subject matter "as a whole." W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984). All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

The references combined by the Examiner in his §103 rejection of claim 2 fail to teach, alone or in combination, all of the limitations recited in claim 2 (as currently amended). The calculation of the inner product is discussed in the references is between

vectors factorized from the aggregate matrix and not between user data vectors being compared vis-à-vis each user as disclosed in the present Application. Furthermore, the centralized calculation for generating recommendations or predictions disclosed in the references teaches away from the distributed calculation of the inner product for calculating similarity that is taught by the Applicants. A prima facie case of obviousness may be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. In re Geisler, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997).

Therefore, it is respectfully suggested that the combining the references to cover all of the limitations of the claim 2 would not have been obvious to one ordinarily skilled in the art. To boil the analysis down to a comparison of calculating inner products with no regard for what products result, how the calculation is performed and to what purpose, impermissibly distills the invention down to a "gist" or "thrust", disregarding the requirement of analyzing the subject matter "as a whole." For these reasons, the applicants respectfully request that the Examiner withdraw his §103(a) rejection of claim 2. Claims 2 and 3 depend from claim 1 and are allowable for at least the same reasons.

Accordingly, the application and claims are believed to be in condition for allowance, and favorable action is respectfully requested. No new matter has been added.

If any issues remain which may be resolved by telephonic communication, the Examiner is respectfully invited to contact the undersigned at the number below, if such will advance the application to allowance.

The Commissioner is authorized to charge Deposit Account 14-1431 in the amount of $210.00 for the extra independent claim (claim13) not previously paid for.

Favorable action is respectfully requested.

Respectfully submitted,

/PETER C MICHALOS/
Peter C. Michalos
Reg. No. 28,643
Attorney for Applicants
(845) 359-7700

Dated: February 19, 2008

**NOTARO & MICHALOS P.C.**
100 Dutch Hill Road, Suite 110
Orangeburg, New York 10962-2100

**Customer No. 21706**

**Mail all correspondence to:**
Yan Glickberg, Registration No. 51,742
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9618
Fax: (914) 332-0615